Det skjer ikke meg ...

Cyberangrep – før, under og etter

God motstandsevne, som handler om både teknologiske og organisatoriske tiltak, er nødvendig for å stå best mulig rustet mot et cyberangrep. Det holder ikke å ansette verdens beste IT-spesialist dersom resten av virksomheten mangler kunnskap om trusler, risiko og sårbarhet i cyberdomenet. Det er ikke et spørsmål om **hvis** virksomheten blir rammet av cyberangrep, men **når**.

Manager
Anna Låstad
Cyber Risk Services, Deloitte

Anna hjelper kunder med beredskap, cyberrespons og forretningskontinuitet – før, under og etter reelle hendelser og kriser.

Manager
Synne Røstgård
Cyber Risk Services, Deloitte

Synne hjelper kunder med å gjennomgå og forbedre sin evne til å håndtere hendelser og virksomhetskriser med utspring i cyberhendelser.

Risikoen for å bli rammet av et cyberangrep

Den digitale trusselen er mer aktuell enn noen gang. Teknologien er i en ekstrem utvikling hvor nærmest alt som går på strøm kobles til internett. Digitaliseringen fører til at angrepsflaten blir større og mer kompleks, og konsekvensene av cyberangrep øker i samme takt. Konsekvensene kan omfatte alle domener; finansielle, strategiske, operasjonelle, etiske, politiske, omdømme, miljø, liv og helse, lov og reguleringer. De kan forårsake ringvirkninger ut i verdikjeder og industrier, i tillegg til å ramme enkeltindivider og samfunnskritiske funksjoner.

Selv om de sikkerhetsmessige utfordringene knyttet til den teknologiske utviklingen har fått en betydelig større oppmerksomhet hos mange virksomheter, skjer utviklingen raskere enn man evner å sikre den. Det er lenge siden man kunne installere et antivirusprogram og tenke at dette ville forhindre at virksomheten ble rammet av et cyberangrep. Bedrifter må evne å beskytte sin data samtidig som de må styrke kunnskapen til de ansatte som bruker systemene. I dag er ingen immune. Risikoen for å bli et offer er stor, og det kreves derfor kontinuerlig fokus for å minimere sannsynligheten for vellykkede angrep. Samtidig må virksomheter konsentrere seg om å redusere konsekvensene dersom de likevel skulle bli et offer. Det finnes ingen enkel løsning eller «silver bullet» som gir en 100 % beskyttelse. Cyberkriminelle blir stadig mer profesjonaliserte og målrettede.

Angrepsmetoder

Det finnes mange ulike varianter av cyberangrep, og det utvikles stadig nye metoder. For å gjennomføre et angrep må det finnes en vei inn, altså et sikkerhetshull. Angrep starter ofte via sårbarheter i nettverket, tredjeparter eller *phishing*. La oss gå gjennom noen eksempler på angrep.

Phishing

Den enkleste veien inn i datasystemet er som regel ved å gå via mennesket, ofte omtalt som «det svakeste ledd». Fremgangsmåten kan være phishing, hvor hackeren manipulerer et menneske til å utføre en handling, eksempelvis til å klikke på en skadelig lenke i en epost eller å betale en falsk faktura. Dette er en form for *sosial manipulasjon* som oftest skjer via epost.

I 2020 ble investor, forretningskvinne og TV-personlighet, Barbara Corcoran offer for *whaling*. Metoden er en variant av phishing der angriperen utgir seg for å være en spesifikk person i en viktig posisjon med særskilte rettigheter. I dette tilfellet utga angriperen seg for å være Barbaras sekretær og sendte en forespørsel til Barbaras regnskapsfører om å overføre 400 000 USD til en konto. Regnskapsføreren gjennomførte overføringen i god tro ettersom eposten tilsynelatende kom fra en person som regnskapsføreren hadde tillit til. Dermed var beløpet tapt. Saken viser hvor viktig det er med bevisstgjøring, god sikkerhetskultur og opplæring av ansatte slik at de er best mulig rustet til å gjenkjenne forsøk på phishing. Prinsippet om telefonisk bekreftelse ved overføring av høye beløp kunne forhindret det vellykkede angrepet i eksemplet over.

Jo mer forberedt man er på et cyberangrep, desto bedre vil man håndtere det.

Løsepengeangrep

En av de mest kjente og alvorligste angrepsmetodene kalles *løsepengeangrep*, *løsepengevirus* eller *digital utpressing,* fra engelsk *ransomware*. Ved slike angrep kommer angriperen seg som regel inn i datasystemet ved bruk av phishing, men kan også få tilgang gjennom å knekke passord eller å finne sårbarheter i et nettverk. Angriperen vil ofte operere uoppdaget og eskalere sine egne rettigheter over tid. Dersom nettverket ikke er sikret tilstrekkelig, vil angriperen lettere kunne bevege seg rundt og hente ut sensitive data som kan brukes til trusler om publisering. Dersom angriperen i tillegg har distribuert skadevare, kan vedkommende kryptere hele eller deler av innholdet på datamaskinen. Et angrep som inkluderer både kryptering og utpressing gjennom publisering av dokumenter, kalles *«double extortion»*. Videre krever angriperen betaling for å unnlate publisering av sensitiv data og/eller for at offeret skal få tilbake tilgang til innholdet. Målet med denne typen angrep er som regel økonomisk vinning, men det kan også være fremmede stater eller konkurrerende virksomheter som ønsker å skade eller å få innsikt i bedriften.

I desember 2021 ble Nordic Choice Hotels rammet av et løsepengevirus. Angrepet skjedde ved at angriperen hadde fått tilgang til systemene hos en tredjepart og koblet seg videre inn i en epost-korrespondanse mellom tredjeparten og Nordic Choice. Angriperen tok over korrespondansen og sendte en epost med et skadelig vedlegg til den ansatte i Nordic Choice. Vedkommende åpnet vedlegget i god tro. Et løsepengevirus spredte seg og medførte at de ansatte ikke kunne håndtere reservasjoner og inn- og utsjekkinger, i tillegg til at funksjonen for å lage nye romnøkler var utilgjengelig. Løsningen ble å kutte nettilgang og stenge ned datasystemene.

Verdikjedeangrep

Angrepsmetode og offer kan være forhåndsbestemt og nøye planlagt før hackeren angriper. Det finnes også flere tilfeller hvor offeret enten er helt tilfeldig, eller en brikke i et spill for å ramme et større hovedmål. Sistnevnte kalles et *verdikjedeangrep* og går ut på at hackeren først angriper en underleverandør eller samarbeidspartner for å komme seg videre inn i datasystemet til en større virksomhet.

Et eksempel på et vellykket angrep gjennom verdikjede og tredjeparter, er Solarwinds i 2020. Solarwinds er et amerikansk IT-firma som tilbyr produkter til overvåkning og håndtering av kritisk IT-infrastruktur. De har over 300 000 kunder, blant annet Oljefondet, flere amerikanske føderale etater og omtrent samtlige av selskapene i Fortune 500. Angriperne klarte å knekke et passord og skaffe seg tilgang til en konto hos Solarwinds. Herfra kunne angriperne eskalere sine rettig-

heter, og de klarte etter hvert å implementere en ondsinnet kode i en programvareoppdatering som skulle sendes ut til alle kunder. Angriperne fikk dermed en bakdør inn til alle kundene som installerte programvareoppdateringen. Angrepet startet i september 2019 og ble først oppdaget i mars 2020. Selv om denne sårbarheten ble lukket av Solarwinds, er det ennå uklart om angriperne fortsatt har tilgang gjennom bakdører som ble laget før angrepet ble oppdaget.

Hva kan gjøres for å øke motstandsdyktigheten?

Det kan oppleves overveldende for en bedrift å skulle sette seg inn i hvordan datasikkerheten kan forbedres og iverksette nødvendige tiltak for å beskytte seg mot cyberangrep. De fleste virksomheter har allerede dimensjonerende rammeverk de må forholde seg til for å tilfredsstille ulike krav, lover og regler. På toppen av dette kommer tiltakene for å for å forsvare seg mot cybertrusler.

Nasjonal Sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet er et aktuelt og nyttig sted å starte. Grunnprinsippene er relevante for alle offentlige og private bedrifter i Norge og handler i hovedsak om teknologiske og organisatoriske tiltak. De omfatter kategoriene *identifisere og kartlegge* (1), *beskytte og opprettholde* (2), *oppdage* (3) og *håndtere og gjenopprette* (4). Alle kategoriene må legges til grunn i arbeidet med å forberede virksomheten på å håndtere et angrep.

Identifisere og kartlegge

Som et første ledd i å øke motstandsdyktigheten bør alle bedrifter ha et bevisst forhold til den konteksten bedriften opererer i. Dette gjør det lettere å vurdere hvilket modenhetsnivå en skal legge seg på, definere målsettinger og kartlegge risikoen bedriften står overfor. Med den raske teknologiske utviklingen – i tillegg til geopolitiske spenninger – er trusselbildet stadig i endring. Virksomheten må derfor sørge for å ha et oppdatert trusselbilde. Bedriften bør kartlegge sin kjernevirksomhet og identifisere prosesser som er kritiske for sentrale oppgaver og funksjoner. I kartleggingen må prosessene kategoriseres ut fra kritikalitet og alle avhengigheter identifiseres, slik at maksimal nedetid kan defineres. Det inkluderer også verdikjeder. Dette hjelper bedriften med å stille tydelige krav internt og eksternt, gir oversikt over kritiske prosesser og toleransen for nedetid. Dette vil gi virksomheten mulighet til å utarbeide alternative måter å holde driften i gang på dersom en hendelse skulle oppstå. Dette er et tidkrevende arbeid, og prosesseiere kan være uenige i hvilke prosesser eller systemer som er viktigst. Midt i en krise vil det være unødvendig ressurskrevende å finne ut av dette. Motstandsdyktighet krever toppledelsens støtte og kontinuerlig fokus. Dersom bedriften er villig til å gjøre denne investeringen, vil gevinsten ved en hendelse være betydelig mindre alvorlige konsekvenser.

Beskytte og opprettholde

Det handler også om å implementere nødvendige sikkerhetstiltak på bakgrunn av bedriftens risikobilde for å kunne skape en solid sikkerhetsorganisasjon. En tilnærming som tar trusselen på alvor, i kombinasjon med en god plan for å håndtere et cyberangrep, vil gjøre bedriften bedre rustet til å begrense skade og gjenopprette normaltilstand.

Mange bedrifter velger å bruke eksterne tjenesteleverandører av IT-tjenester. Dette må likevel ikke føre til en ansvarsfraskrivelse i bedriften når det gjelder sikkerheten. I disse tilfellene må virksomheten kartlegge tjenesteleverandørens sikkerhet, forankre leveranser i kontrakt og ha en kontinuerlig oppfølging av leverandøren. Et eksempel er å avdekke hvem fra tjenesteleverandørens side som har innsyn i bedriftens informasjon, hvordan denne informasjonen behandles og lagres, samt hvordan informasjonen skilles fra tjenesteleverandørens andre kunder. Ofte kan det være hensiktsmessig å inkludere leverandøren i øvelser.

Oppdage

Det er flere metoder som kan bidra til å oppdage forsøk på cyberangrep. Overvåkning av nettverkstrafikk og gjennomgang av sikkerhetslogger er eksempler på tiltak som kan utføres, enten av interne eller eksterne tekniske ressurser. Det er viktig at ressursene har riktig kompetanse for å kunne oppdage inntrengingsforsøk på en effektiv måte. En annen fremgangsmåte er å skape en god sikkerhetskultur gjennom bevisstgjøring av de ansatte. Dette krever opplæring på alle nivå i organisasjonen. Det gjelder å skape bevissthet rundt både brukeratferd og sårbarhet, og vise den enkelte ansatte hvorfor akkurat deres handlinger kan bidra til å stoppe angrep. Det må også bygges en forståelse for konsekvensene av et cyberangrep. Dette gjelder ikke bare for bedriften, dens samfunnsoppdrag og kunder, men også for hver enkelt ansatt. Et uheldig tastetrykk på et skadelig vedlegg kan få alvorlige konsekvenser.

Det er lett å la seg lure av hackernes profesjonalitet og stadig mer sofistikerte angrep. Oljefondssjef Nicolai Tangen uttalte seg offentlig om hvordan han selv lot seg lure av utspekulerte hackere som fikk kontroll over maskinen hans. Dette var ikke et ondsinnet angrep, men heldigvis bare en sikkerhetstest som var arrangert av sikkerhetsteamet i hans egen organisasjon.

Håndtere

For å skape en god beredskap i virksomheten er det avgjørende å utarbeide et planverk for krisehåndtering på strategisk nivå, i tillegg til cyberrespons, forretningskontinuitet og gjenoppretting på operasjonelt nivå. Planverket må beskrive en tydelig fremgangsmåte som er enkel å følge, klar rolle- og ansvarsfordeling, klassifisering av hendelser, prioritering av oppgaver og rutiner for kommunikasjon. Planverket skal fungere som et svar på det som ble nevnt under «identifisering og kartlegging».

Likhetsprinsippet

Likhetsprinsippet er et av hovedprinsippene for beredskapsarbeid og innebærer at krisehåndteringen bør ha tilsvarende linjeorganisering og være mest mulig lik daglig struktur for å unngå forvirring. Dette henger også sammen med utarbeidelse av rolle- og ansvarsbeskrivelse for personellet som skal

involveres i krisehåndteringen. Personellet bør bestå av ledere med beslutningsansvar og nøkkelpersoner som har sentrale oppgaver i bedriften. Dette henger igjen sammen med *ansvarsprinsippet* som går ut på at daglige roller og funksjoner skal ivaretas under en krise. De som kjenner fagområdet i normalsituasjon, vil sannsynligvis ha bedre forutsetning for å forstå omfanget og fatte gode beslutninger under en krise.

Gjør planverket kjent
Det er viktig at planverket er kjent, oppdatert og tilgjengelig for relevante roller når uhellet først er ute. Derfor vil det være nødvendig at kriseteamet har trent på å håndtere et cyberangrep. Håndteringen kan pågå i alt fra dager, til uker og måneder. Det er en svært krevende situasjon å stå i, og for mange en stor påkjenning og belastning – både psykisk og fysisk. For å håndtere hendelsen best mulig er det nyttig å ha vært gjennom dette tidligere, i form av trening og øvelser. Kunnskap om prosessen vil øke personellets trygghet, samtidig som at det kan være med på å sikre at planverket følges. Øvelser vil også kunne avdekke om det finnes hull i planverket og bidra til oppdatering av dette. Har kriseledelsen tilstrekkelig kompetanse til å forstå kriser som har oppstått i cyberdomenet?

Opprettholdelse av driften
Forretningskontinuitet skal sørge for at virksomheten kan opprettholde drift, selv under driftsforstyrrende hendelser. Krisehåndtering dreier seg om strategisk håndtering av kriser, mens cyberhendelseshåndtering skal sørge for at cyberhendelser blir håndtert på en effektiv måte på operasjonelt nivå. En viktig ting å tenke på, er hvilke roller eller nivå som skal sitte med de ulike mandatene. Har leder av cyberresponsteamet mandat til å skru av bedriftens IT-systemer eller skal dette avgjøres av strategisk kriseledelse? Hvem skal avgjøre hvorvidt løsepenger skal betales? Bør styret involveres? Mange velger å utarbeide spesifikke «playbooks» for sine største cyberrisikoer. Dette blir da en oppskrift på hvordan man skal håndtere en spesiell hendelse, for eksempel tap av sensitive data eller løsepengeangrep.

Når angrepet først har skjedd …

… går minuttene fort. Usikkerhet og potensielle negative innvirkninger kan føre til at det er mange følelser i spill, og den ustabile situasjonen kan skape alt fra uro til panikk. Det er avgjørende å sikre trygghet for virksomhetens ansatte og interessenter, samtidig som det settes i gang tiltak så fort som mulig for å stoppe angrepet og redusere skadene. For å kunne håndtere krisen raskt og målrettet, er *kommunikasjon* en nøkkelfaktor. Kriseteamet må ha en god dialog for å kunne etablere en *felles situasjonsforståelse*. Dette er helt avgjørende for å arbeide sammen mot et felles mål. Her gjelder det å skape forståelse for hva som hittil har skjedd og hva bedriften står overfor. Det kreves et tilpasningsdyktig kriseteam med en situasjonsbetinget ledelse. Situasjonen kan endre seg kjapt, og informasjon må deles fortløpende for å ivareta en dynamisk situasjonsforståelse.

Kartlegging av tiltak
Teamet må også ta i bruk planverket og kartlegge hvilke tiltak som skal iverksettes for å få kontroll på hendelsen, hindre spredning og minimere konsekvensene. Under et angrep kan virksomheten miste tilgang på alle data, eller risikere at angriperen overvåker samtlige systemer. Man bør derfor unngå å bruke kommunikasjonsverktøy på bedriftens IT-system under en krise, som epost, chat, videokonferanser, intranett og lignende. Før hendelsen er det derfor lurt å implementere alternative kommunikasjonskanaler som er uavhengig av bedriftens IT-system. For å skape en mer effektiv krisehåndtering, kan planverket med fordel inneholde retningslinjer og forhåndsbestemte handlingsmønstre.

En åpen og transparent kommunikasjon
Det anbefales også å ha en åpen og transparent *kommunikasjon* under krisen, både internt i virksomheten og eksternt opp mot interessenter og media. En lukket håndtering kan føre til større usikkerhet og tap av omdømme. Norsk Hydro er et godt eksempel på åpenhet under en krise. Da de ble rammet av et massivt cyberangrep i 2019 som kostet dem ca. 600 millioner kroner, var strategien å dele så mye informasjon som mulig både internt og eksternt. Det ble blant annet avholdt jevnlige pressekonferanser og daglige allmøter som ble sendt på video til lokasjoner globalt, for å holde ansatte, kunder og media orientert. Den åpne håndteringen skapte internasjonal oppsikt. Som første private virksomhet, mottok Hydro Kommunikasjonsforeningens Åpenhetspris for 2019.

Gjenoppretting

Planer for gjenoppretting skal sørge for at prosesser blir gjenopprettet i en prioritert rekkefølge, helt ned til IT-infrastruktur og maskinvare. Dette bør koordineres av et team sammen med de ulike prosess- og systemeierne. Når isolering og etterforskning av hendelsen er gjennomført, kan arbeidet med å gjenopprette og returnere til normal tilstand starte. Veien mot dette punktet kan være utfordrende, for når vet du egentlig om du kan stole på systemene dine? Hvor lenge har angriperen hatt tilgang? Noen ganger finner man svaret, mens man andre ganger må leve med usikkerheten.

Planlegge på forhånd
Gjenoppretting etter et stort cyberangrep kan ta lang tid dersom man ikke har utarbeidet en god plan på forhånd. I enkelte tilfeller er det nødvendig å anskaffe ny maskinvare, noe som ikke er like enkelt lenger. Mangel på grunnstoffer, ettervirkninger av pandemien og høy etterspørsel gjør at produsentene ikke klarer å dekke behovet for flere nødvendige komponenter.

Evaluere angrep og håndtering
Etter et cyberangrep er det viktig å gjøre en grundig evaluering av angrepet og håndteringen. Ved å trekke ut læringspunkter fra hendelsen, vil virksomheten kunne avdekke hull eller forbedringer i planverket og gjøre virksomheten bedre forberedt på et eventuelt fremtidig angrep. Gjennomgangen vil også kunne skape forståelse av krisen, håndteringen

og skadeomfanget. Samtidig vil det være nyttig for andre virksomheter å lære. Erfaringen kan også tjene som en realitetsvekker for andre bedrifter. Til tross for en ekstrem økning i cyberhendelser, finnes det fortsatt bedrifter som anser sannsynligheten for å bli angrepet som liten. Klassikeren «det skjer ikke oss» lever fortsatt. Heldigvis opplever konsulentbransjen en større pågang fra bedrifter som forstår alvoret og investerer i sikkerhetstiltak for å forbedre beredskapen opp imot cyberhendelser. Dette er kontinuerlig arbeid som krever tid og ressurser.

Ble berømmet for åpenheten

Tidligere konserndirektør for Kommunikasjon & Myndighetskontakt i Norsk Hydro, Inger Sethov, uttalte at cyberangrepet mot Hydro i 2019 var den mest utfordrende krisen hun hadde håndtert i løpet av sin karriere. Et av læringspunktene Hydro satt igjen med etter angrepet, var overraskelsesmomentet de opplevde. Hun uttrykte at man vil bli overrasket under et angrep, uavhengig av om man planlegger og trener på det. Heldigvis er ikke cyberangrep annerledes enn andre uventede kriser som oppstår: Jo mer forberedt man er på et cyberangrep, desto bedre vil man håndtere det.

Bærekraftsbegreper og et blikk fremover

I denne artikkelen ønsker vi å bidra til økt forståelse for hvilke rammeverk som finnes, hvordan bærekraftsrapporteringen vil se ut fremover, og hvordan virksomhetene kan navigere seg frem i rapporteringsjungelen.

M.Sc Industriell Økologi
Dorthea Vollset Almklov
Konsulent i Climate Change and Sustainability Services, EY

Siviløkonom
Henriette Andreassen
Senior konsulent i Climate Change and Sustainability Services, EY

Siviløkonom
Julia Furulund Jakobsen
Konsulent i Climate Change and Sustainability Services, EY

Det er lett å gå seg vill i en rapporteringsjungel som stadig blir tettere. Utallige nye rammeverk og forkortelser medfører utfordringer for virksomheter som ønsker å løfte bærekraftsrapporteringen til et nytt nivå for å opptre transparente om ikke-finansielle risikoer og muligheter i virksomheten fremover. I bærekraftsammenheng er en frodig jungel som regel positivt, men ikke når det kommer til en jungel av antall standarder å rapportere etter.

En jungel av rammeverk og initiativer

I 2014 kom *EUs Non-Financial Reporting Directive (NFRD)*[1] som pålegger store børsnoterte selskaper med over 500 ansatte å rapportere på ikke-finansiell informasjon som omhandler miljø og sosiale forhold, som for eksempel respekt for menneskerettigheter, antikorrupsjon og mangfold i ledelsen. EU-direktivet er også tatt inn i norsk lov gjennom *regnskapsloven 3-3c* som forplikter store norske bedrifter å redegjøre for samfunnsansvar i styrets årsberetning. Det er imidlertid ingen obligatorisk standard for hvordan denne informasjonen skal rapporteres, verken i Norge eller EU. Dette har ført til en jungel av initiativer og frivillige standarder for rapportering. Nedenfor vises en oversikt over formålet med de ulike rammeverkene og initiativene, og hvem som med fordel kan ta utgangspunkt i disse i sin bærekraftsrapportering.

Global Reporting Initiative (GRI)

Formål

Å skape et felles språk for ulike selskaper og deres interessegrupper, hvor de økonomiske, miljømessige og sosiale konsekvensene av virksomhetens drift kan kommuniseres og forstås.

Relevans

GRI utformet den første globale standarden for bærekraftsrapportering i 1997 og er den mest brukte standarden for bedrifter i Norge og EU. GRI består av standarder for rapportering av vesentlige påvirkningsområder innen økonomiske, miljømessige og sosiale aspekter. I fjor ble GRI-standardene oppdatert med endringer av noen av indikatorene. Rammeverket består i dag av tre universelle standarder (GRI 1, 2 og 3) som kan benyttes av alle typer virksomheter, og et sett med sektorspesifikke standarder. GRI 1 inneholder krav og prinsipper for bruk av GRI-standardene og legger dermed grunnlaget for bærekraftsrapporteringen. GRI 2 inneholder retningslinjer

[1] Directive 2014/95/EU.